

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION**

UNITED STATES OF AMERICA,

Plaintiff,

v.

NICHOLAS H. HAGLOF,

Defendant.

)
)
)
)
)
)
)
)
)
)

Cause No. 4:20-CR-00384 HEA/SPM

**DEFENDANT’S REPLY TO GOVERNMENT’S MEMORANDUM
REGARDING DEFENDANT’S MOTION PURSUANT TO FEDERAL RULE OF
CRIMINAL PROCEDURE 17(c)**

Comes now Counsel for Defendant, Nicholas Haglof, and respectfully replies to Government’s Memorandum Regarding Defendant’s Motion for a Subpoena Pursuant to Federal Rule of Criminal Procedure 17(c). Furthermore, Defendant respectfully requests that the Court issue subpoenas to both Microsoft – Online Operations and the National Center for Missing and Exploited Children for documents relevant to the investigation of Defendant’s IP address which forms the basis of the search warrant for Defendant’s residence. In support of this motion, Defendant offers the following:

FACTUAL BACKGROUND

1. Defendant incorporates as reference the Factual Background listed in his Motion for a Subpoena Pursuant to Federal Rule of Criminal Procedure 17(c). (Doc. 38).
2. The basis of the search warrant in this case is a “Cyber Tip” received by the National Center for Missing and Exploited Children (NCMEC) from Microsoft Inc – Bing Images. *See* Exhibit 1. Bing, a subsidiary of Microsoft, allegedly identified child pornography being searched

through their photo search system by an electronic device later found to be associated with Defendant's IP address.

3. According to the Cyber Tip, Microsoft/Bing identified these suspect images using specialized software that scans their servers looking for child pornography. This program is called PhotoDNA.

4. PhotoDNA was developed between a partnership with Microsoft, NCMEC, and Dartmouth College after NCMEC approached Microsoft and asked them to develop a program to seek, identify, and report child pornography on the internet. PhotoDNA is provided to other electronic service providers by Microsoft through NCMEC.

5. On April 6, 2021, Defense Counsel sent a request for discovery to the Government seeking the items that are the subject of this motion. The request was targeted to confirm the use of Microsoft's PhotoDNA program in this case, to learn the identity of those who operated it, to evaluate policies and procedures related to its use, and to examine partnership agreements between Microsoft, NCMEC, and law enforcement pertaining to the use of PhotoDNA.

6. On April 28, 2021, the Government responded in writing through Assistant U.S. Attorney Jillian Anderson that:

“In reference to your April 6, 2021, letter requesting six additional items of information in *USA v. Haglof*, please be aware that neither we nor the law enforcement officers and agents that worked on Mr. Haglof's investigation are in possession of the information you seek regarding the personnel and operations of Microsoft Corp. or the personnel and programs utilized by the NCMEC. *I do believe you may be able to get the information you seek from NCMEC or Microsoft.*” (emphasis added).

7. Now that Defendant seeks to obtain a subpoena pursuant to Rule 17(c) to do the very thing the Government suggested, the Government objects to the issuance of that subpoena.

LEGAL AUTHORITY & ARGUMENT

I. The Government lacks standing to object to Defendant's request for subpoena.

When challenging the issuance of a subpoena under Rule 17(c), the Government has the burden of demonstrating it has standing. *See KVOs, Inc. V. Associated Press*, 299 U.S. 269, 278 (1936); *Scott v. Breeland*, 792 F.2d 925, 927 (9th Cir. 1986); *United States v. Tomison*, 969 F.Supp. 587 (E.D. Cal. 1997) (holding that because standing goes to the jurisdiction of the Court, the Government as the party attempting to invoke that court's jurisdiction has the burden of demonstrating it has standing).

A party only has standing to move to quash the subpoena issued to another when the subpoena infringes upon the movant's legitimate interests. *See United States v. Raineri*, 670 F.2d 702, 712 (7th Cir. 1982); *Ponsford v. United States*, 771 F.2d 1305, 1308 (9th Cir. 1985). "In many instances the opposing party in a criminal case will lack standing to challenge a subpoena issued to a third party because of the absence of a claim of privilege, or absence of a proprietary interest in the subpoenaed documents." *United States v. Reyes*, 162 F.R.D. 468, 471 (S.D.N.Y. 1995). Accordingly, the Government lacks standing to raise the exclusive grounds for quashing a subpoena because it has no injury in fact relative to a claim of privilege or proprietary interest. *See Gladstone Relators v. Bellwood*, 411 U.S. 91, 99 (1979); *Tileston v. Ullman*, 318 U.S. 44, 46 (1943) (no standing to raise third party's injury); *Tomison*, 969 F.Supp. at 594 (government lacks standing to object to product of documents in third party possession when they cannot claim privilege); *Compare United States v. Vasquez*, 258 F.R.D. 68 (E.D.N.Y. 2009) (holding government did have standing to object under Rule 17(c) to documents held by a county law enforcement agency that would relate to law enforcement privilege of federal agents); *United States v. Louis*, 2005 WL

180885 at *5 (S.D.N.Y. Jan. 27, 2005) (government standing to quash where documents held by federal government agency that assisted in underlying criminal investigation).

In this case, the Government lacks any claim of privilege or proprietary interest in the material sought so they lack standing to object. The very essence of the Government's objection is neither Microsoft nor NCMEC are Government actors, and neither colluded with the Government to develop/operate any software to detect child pornography or acted in any other way that would give rise to an infringement upon Defendant's rights because the initial cyber tip investigation was all undertaken by Microsoft on their own initiative. If this is true, then there can be no privilege or proprietary interest on behalf of the Government. Any claim to the contrary would support Defendant's Motion for a Subpoena and anticipated Motion to Suppress. Given that the Government lacks standing to object, the Court should issue the subpoenas requested.

II. Defendant meets the criteria for the issuance of a subpoena under Rule 17(c), and the request is within the scope of the rule.

A criminal defendant has a constitutional right to obtain evidence and a right to process. *California v. Trombetta*, 467 U.S. 479, 485 (1984); *Brady v. Maryland*, 373 U.S. 83, 87 (1963). Rule 17(c) implements both the right to obtain testimonial or documentary evidence and the right to require its production. *Id.* The right to this evidence and testimony to challenge not just the facts that go towards guilt or punishment, but the right to obtain evidence for trial. The federal discovery rules go even further, encompassing the right to explore violations of search and seizure. *See United States v. Soto-Zuniga*, 837 F.3d 992, 1000-01 (9th Cir. 2016) (finding that rule 16(a)(1)(E) permits discovery related to the constitutionality of a search and seizure).

While Rule 17(c) is not to be used as a broad discovery device, it can be used in a good-faith effort to obtain evidence subject to the factors set forth in *United States v. Nixon*, 418 U.S. 683 (1974). The *Nixon* factors require the defense to demonstrate that the materials are: 1) relevant, 2) admissible, 3) specifically identified, and 4) not otherwise procurable. *Id.* at 698-699.

The Eighth Circuit Court of Appeals has utilized the *Nixon* factors when addressing the propriety of a Rule 17(c) subpoena directed to a third party. *United States v. Hang*, 75 F.3d 1275, 1283 (8th Cir. 1996); *United States v. Stevenson*, 727 F.3d 826, 831 (8th Cir. 2013). However, neither *Hang* nor *Stevenson* stand for the proposition that criminal defendants are to be summarily denied the use of a subpoena to obtain material for the defense or that the *Nixon* standards are absolute when dealing with third parties. *See Hang*, 75 F.3d at 1283 (discussing the application narrowly to the issue of psychotherapist privilege when defendant provided zero grounds for discovery); *Stevenson*, 727 F.3d at 831 (indicating that because defendant failed to seek a broader standard under Rule 17(c) review for a subpoena directed at a third party, *Nixon* factors applied).

The Government's claim that the material sought is not clear or precise enough to allow the parties here to determine what Defendant seeks is untrue. The request asks specific questions related to the name of the employees at Microsoft and NCMEC who worked on this investigation, the name of the computer programs used, written agreements between Microsoft and NCMEC related to this narrow topic, and the policies and procedures for executing the very investigation that was done in this case. The Government is aware that these requests are targeted to get at the very heart of the issue addressed in the cases they cite. That is: 1)

establishing that Microsoft partnered with law enforcement to combat child pornography, and 2) Microsoft acted at the behest of the Government in doing so. While the Defendant cannot specifically identify all material with one hundred percent precision, the request is still specific enough to allow for Microsoft and NCMEC to know that is sought. The Defendant asks the Court to recognize the impossible position Defendant is in when attempting to obtain material from an entity that keeps the material relatively secret. Nevertheless, in this case, enough is known to seek a subpoena (addressed in detail in Section III).

To combat Defendant's request, the Government's relies on *Stevenson* and *Richardson* which are both distinguishable. In *Stevenson*, the Eighth Circuit Court of Appeals upheld a district court denial of a subpoena to AOL pursuant to Rule 17(c) in a child pornography investigation where the defendant sought to establish a connection between AOL and the Government by requesting information related to their file-scanning software and partnership agreements. 727 F.3d at 830. However, the Eighth Circuit only upheld this decision *after* the record established, through the testimony of AOL's Director of Investigations & Cyber Security, that 1) AOL developed its file-scanning program without prompting or input from any government agency, 2) AOL did so primarily to protect its network, and 3) AOL operating its file-scanning program independently of any government program. *Id.*

In this case, the Government has offered no such evidence or testimony to support this is the case with Microsoft. On the contrary, Defendant will establish that unlike AOL, both Microsoft and NCMEC worked together to create file-scanning software. It is important for this Court to note that NCMEC is a government entity. See *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016) (the Tenth Circuit Court of Appeals held in an opinion written by now

U.S. Supreme Court Justice Neil Gorsuch that NCMEC was a government entity). The *Ackerman* court found that NCMEC's statutory authority under 18 U.S.C. § 2258A and 42 U.S.C. § 5773(b), which require it to maintain a tipline and investigate tips for suspected child pornography, qualify the center as a government entity. *Id.* The post-*Ackerman* cases cited by the Government all primarily accept this as a fact.

The *Ackerman* decision is significant here because the *Stevenson* decision predates this decision. Now that more is known about NCMEC, its governmental role, and its cooperation with electronic service providers like Microsoft, the *Stevenson* decision should be re-examined. That is exactly what the Defendant seeks the Court to do in this case.

The Government's reliance on *United States v. Richardson*, 607 F.3d 357 (4th Cir. 2010) also suffers from similar defects. *Richardson* also involves a defendant's attempts to subpoena AOL material related to their child pornography file-screening software and investigations. *Id.* The Fourth Circuit found that the defendant's attempts to obtain all records relating to AOL's coordinated efforts with law enforcement to be overbroad and unduly burdensome because the defendant's request was not specific in any way and sought items like *all* emails, postal correspondence, and meeting notes between anyone at AOL and anyone in law enforcement. *Id.* at 362-63. The volume of material and lack of specificity was insufficient for a subpoena. *Id.*

Like in *Stevenson*, the Fourth Circuit also focused on the written declaration from an AOL executive which swore that they were not working with the Government and developed the file-screening software to protect their network. *Id.* Here again, the Government asks the Court to deny Defendant's subpoena request while offering no evidence to support it. Also, the *Richardson* case was decided before *Ackerman* which uncovered NCMEC's close relationship

with electronic service providers and found that NCMEC is an arm of the Government. *Ackerman*, 831 F.3d at 1297-99.

The material requested by Defendant meets the requirements of Rule 17(c) and is within the scope of the rule. When seeking to make a claim that a private actor conducted a search as an instrument or agent of the Government, a defendant shoulders the burden of establishing the existence of an agency relationship, which is “a fact-intensive inquiry guided by common law agency principals.” *United States v. Ellyson*, 326 F.3d 522, 527 (4th Cir. 2003); *United States v. Jarrett*, 338 F.3d 339, 344 (4th Cir. 2003). The degree that a private actor performs a search for the Government “necessarily turns on the degree of the Government’s participation in the private party’s activities.” *Skinner v. Ry. Labor Execs.’ Ass’n*, 489 U.S. 602, 613-14 (1989); *See also United States v. Highbull*, 894 F.3d 955, 991-92 (8th Cir. 2018). There must be some evidence of Government participation in the private search before a court can hold the private search unconstitutional. *Jarrett*, 338 F.3d at 346.

The evidence sought in this case is narrowly tailored to seek information from the private party – Microsoft – that will show its level of involvement in file-screening software development and implementation with the Government, NCMEC, and other law enforcement agencies. It is not overbroad or unduly burdensome. This is required for the Defendant to meet his burden of showing the government agency relationship with Microsoft. To deny this request, but to simultaneously require the Defendant to meet the burden of providing evidence to support the “fact-intensive inquiry” required by using documents only in the possession of Microsoft and NCMEC, would be the equivalent of effectively doing away with the private government actor doctrine provided by the Supreme Court in *Skinner*. That is not a just result.

III. Microsoft acts as an agent of the Government when conducting online surveillance to locate and report child pornography.

NCMEC works closely with the Microsoft corporation in fulfilling its Congressional mandate to assist with the criminal prosecution of child pornography cases. *See* 18 U.S.C. § 2258A(a). Microsoft is a United States corporation that develops computer software. One program that Microsoft has developed over the years is a restricted remote computer service called PhotoDNA. According to the discovery provided by the Government, Microsoft was able to search Defendant's Microsoft activity using PhotoDNA, which is why this is relevant in this case.

Microsoft worked in collaboration with NCMEC and Dartmouth College to develop PhotoDNA, a computer program that seizes and searches digital photographs to create a hash value of the images to compare with various libraries of purported child pornography so that it can be reported to NCMEC.¹

Microsoft partners not only with NCMEC, but also with state, national, and even international law enforcement organizations to maximize the evidentiary benefits of the PhotoDNA program for use in criminal prosecutions.² One of the ways that Microsoft partnered with NCMEC and the law enforcement community is in the development of the PhotoDNA program itself.³ Microsoft has provided the PhotoDNA program to NCMEC and access to its platform to law enforcement agencies and select electronic communication service providers at

¹ *See* Ex. 2. Tracy Ith, *Microsoft's PhotoDNA: Protecting Children and Businesses in the Cloud*, MICROSOFT available at <https://news.microsoft.com/features/microsofts-photodna-protecting-children-and-business-in-the-cloud/> (last visited August 9, 2021).

² *Supra* note 1.

³ *Supra* note 1.

no charge.⁴ Microsoft does so in order to streamline the collection of evidence on behalf of law enforcement so child pornography cases can be more easily prosecuted.

Another way that Microsoft collaborates with federal and local law enforcement agencies in the United States, including NCMEC, is by participating in the sharing of hash values.⁵ The Industry Hash Sharing Platform is a database of hash values controlled and maintained by NCMEC. This library of hash values used by the PhotoDNA program is renewed and updated daily by NCMEC so Microsoft can intercept newly identified images of apparent child pornography on the Internet. The constant library update allows entities like Microsoft to swiftly intercept images of apparent child pornography and forward them to law enforcement for prosecution. Finally, Microsoft provides access to the PhotoDNA program free of charge to select electronic communication service providers on the Internet, if those providers handle user-generated content and agree that Microsoft can send the evidence it obtains concerning apparent child pornography to NCMEC and law enforcement for prosecution. *Id.*

In short, Microsoft utilizes its considerable computer programming talents and financial resources as an agent of NCMEC, a known federal law enforcement entity under *Ackerman*, to perform a law enforcement function: locate and identify evidence involving apparent child pornography crimes for prosecution. Therefore, by Microsoft's own admissions in its published website, it has partnered with NCMEC to develop this program.⁶ This website, which features a video of Microsoft executives discussing their collaboration with NCMEC and the article

⁴ Supra note 1.

⁵ See <https://www.microsoft.com/en-us/PhotoDNA/FAQ> (last visited August 9, 2021).

⁶ See Tracy Ith, *Microsoft's PhotoDNA: Protecting Children and Businesses in the Cloud* available at: <https://news.microsoft.com/features/microsofts-photodna-protecting-children-and-businesses-in-the-cloud/> (which contains a video from Microsoft executives discussing their collaborative effort with NCMEC); see also Ex. 3, Hany Farid, *Reining in Online Abuses*, TECHNOLOGY AND INNOVATION, Vol. 19, pp. 593-599 (2018) (PhotoDNA's

published in an academic journal with the same claims, provide a good-faith basis to rebut any argument that Microsoft developed and utilizes the PhotoDNA program “own its own” for “business purposes,” a claim which is critical to the Government’s challenge. *See* Exhibit 4.

This collaboration is evidence to support that Microsoft was a government actor when it conducted its PhotoDNA search of Defendant’s Microsoft activity. This approach converts Microsoft into a government actor and triggers Fourth Amendment protections which were not afforded in this case. This issue will be addressed in a separate motion. In the meantime, the requested subpoena is necessary to support this motion.

This publicized relationship between Microsoft and NCMEC distinguishes this case from the other cases cited by the Government in their response. *See United States v. Bebris*, 2021 U.S. Dist. LEXIS 20974 (7th Cir. 2021) (finding no link between NCMEC and Facebook after hearing testimony from NCMEC that they did not collaborate with Facebook and receiving a declaration from Facebook concerning same); *United States v. Miller*, 982 F.3d 412, 424026 (6th Cir. 2020) (finding no link between NCMEC and Google after receiving a declaration from a Google executive describing how their file-screening system is independent from NCMEC).

The Government cites to *United States v. Ringland* because it is a recent Eighth Circuit case concerning Google reporting Cyber Tips to NCMEC where the defendant claimed Google was a government actor. 966 F.3d 731 (8th Cir. 2020). In *Ringland*, the Eighth Circuit held that the statutory reporting obligation codified in 18 U.S.C. Section 2258A(a), *by itself*, was insufficient to support the government agency over Google. *Id.* at 737. Thus, the Eighth Circuit can be seen as holding that, without *further* evidence, the statutory obligation alone is insufficient. *See also*

developers acknowledges program was developed in cooperation with Microsoft, NCMEC, and Dartmouth College after NCMEC approached Microsoft).

Stevenson, 727 F.3d at 830 (reporting requirement for child pornography alone does not transform the electronic service provider into a government agent). In this case, the subpoena is targeted to address the concerns the Eighth Circuit raised in *Stevenson* and *Ringland* by proving there is greater collusion between the government via NCMEC and Microsoft in the development and execution of PhotoDNA.

Microsoft's Cyber Tips using PhotoDNA have been discussed in *United States v. Reddick*, as cited by the Government. 900 F.3d 636, 638 (5th Cir. 2018). However, *Reddick* does not address the government agency question presented in this case. Instead, the question presented in *Reddick* was whether the law enforcement investigator's subsequent warrantless search of the information provided to him by Microsoft was a significant expansion of the search that had been conducted previously by Microsoft, also known as the private search doctrine. *Id.* The defendant did not raise the *Skinner* government actor challenge, and it was not presented on appeal. This is a completely different legal issue than what is presented here, and therefore *Reddick* is entirely distinguishable.

Therefore, there is ample evidence to support the assertion that Microsoft is a government actor. Subpoenas are necessary to establish this at motions hearings by offering evidence to support the anticipated motion.

IV. Conclusion

The Government's opposition to the Defendant's Motion for Subpoenas lacks standing and should be disregarded. Nothing has been presented that should deny Defendant the right to obtain evidence for a motions hearing. The bulk of the Government's factual basis in their memorandum is wasted on facts trying to establish Defendant's guilt, which is not essential to the Court's determination on this legal issue. This is an attempt to misdirect the Court's attention away from

the legal issue. The Government's legal analysis is largely spent on citing distinguishable cases to ultimately argue that the Defendant's anticipated Motion to Suppress will not prevail, despite offering no evidence to the contrary, and as such, the Court should just "cut to the chase" and deny Defendant's Motion for Subpoena. Yet, based on existing case law and publicly available documentation provided by Microsoft itself, there is more than a good-faith basis to demonstrate Microsoft colluded with Government through NCMEC to support ongoing law enforcement operations and prosecution. This forms a sufficient basis for the narrowly tailored subpoenas requested.

WHEREFORE, for the foregoing reasons, Defendant respectfully requests the Court issue a subpoena pursuant to Federal Rule of Criminal Procedure 17(c) to both Microsoft – Online Operations and the National Center for Missing and Exploited Children for the documents described in Document 38.

Respectfully submitted,

FRANK, JUENGEL & RADEFELD,
ATTORNEYS AT LAW, P.C.

By /s/ Daniel A. Juengel
DANIEL A. JUENGEL (#42784MO)
Attorney for Defendant
7710 Carondelet Avenue, Suite 350
Clayton, Missouri 63105
(314) 725-7777

CERTIFICATE OF SERVICE

I hereby certify that on August 11, 2021, the foregoing was filed electronically with the Clerk of the Court to be served by operation of the Court's electronic filing system upon the following.

Jillian Anderson
Asst. United States Attorneys
111 South Tenth Street, 20th Floor
St. Louis, Missouri, 63102

/s/ Daniel A. Juengel

DANIEL A. JUENGEL